配置Active Directory與Firepower裝置的整合以實 現單點登入&;強制網路門戶身份驗證

目錄
<u>簡介</u>
<u>必要條件</u>
<u>採用元件</u>
<u>背景資訊</u>
<u>設定</u>
步驟 1.配置Firepower使用者代理進行單點登入
步驟 2.將Firepower管理中心(FMC)與使用者代理整合
步驟 3.將Firepower與Active Directory整合
步驟3.1建立領域
<u>步驟3.2新增目錄伺服器</u>
<u>步驟3.3修改領域配直</u> 生團2.4工载点田老姿料度
<u>步驟4.配直身份束略</u> 步驟4.1論制網路門戶(主動身份驗證)
步骤 <u>3.1国的时间门(工业3700000)</u> 步驟4.2單點登入(被動身份驗證)
步驟 5.配置訪問控制策略
步驟 6.部署訪問控制策略
步驟7.監視使用者事件和連線事件
<u>驗證與疑難排解</u>
<u>驗證FMC和使用者代理之間的連線(被動身份驗證)</u>
<u>驗證FMC和Active Directory之間的連線</u>
<u>檢驗Firepower感測器與終端系統之間的連通性(主動身份驗證)</u>
<u>驗證策略配置和策略部署</u>
分析事件日誌
相關資訊

簡介

本文檔介紹強制網路門戶身份驗證(主動身份驗證)和單點登入(被動身份驗證)的配置。

必要條件

需求

思科建議您瞭解以下主題:

- Sourcefire Firepower裝置
- 虛擬裝置型號
- 輕量級目錄服務(LDAP)
- Firepower使用者代理

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Firepower管理中心(FMC)版本6.0.0及更高版本
- Firepower感測器6.0.0及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

強制網路門戶身份驗證或主動身份驗證提示登入頁面,主機需要使用者憑據才能訪問Internet。

單點登入或被動身份驗證為使用者提供無縫的網路資源和Internet訪問身份驗證,而無需多次出現使 用者憑據。單點登入身份驗證可通過Firepower使用者代理或NTLM瀏覽器身份驗證實現。

💊 注意:對於強制網路門戶身份驗證,裝置必須處於路由模式。

設定

步驟 1. 配置 Firepower 使用者代理進行單點登入

本文說明如何在Windows電腦中配置Firepower使用者代理:

安裝和解除安裝Sourcefire使用者代理

步驟 2. 將Firepower管理中心(FMC)與使用者代理整合

登入到Firepower Management Center,導航到System > Integration > Identity Sources。 按一下 New Agent(新代理)選項。配置User Agent系統的IP地址,然後按一下Add按鈕。

按一下Save按鈕儲存更改。

Overview	Analysis	Policies Devices	Objects AN	1P							Deploy	A Sy	stem Help v	admin 🔻
						Configuration	Users	Domains	Integration	Updates	Licenses v	Health +	Monitoring •	Tools •
Cisco CSI	Realms	Identity Sources	eStreamer	Host Input Client	Smart Softwar	e Satellite								
											You have unsaved	d changes	🔀 Cancel	Save
Identity S	ources													
Service Type		None	Identity Services	Engine User Age	nt									
-	User	Agent			2 X	New Agent								
Host Name	/IP USEL	ngent												
	Host	Name/IP Address 192.1	68.10.11											
			(Add Cano	el									

步驟 3.將Firepower與Active Directory整合

步驟3.1建立領域

登入到FMC, 導航到System > Integration > Realm。按一下新增新領域選項。

名稱和說明:提供名稱/說明以唯一標識領域。

文字:AD

AD主域:Active Directory的域名

目錄使用者名稱: <username>

目錄密碼:<password>

基本DN:系統從LDAP資料庫中開始搜尋的域或特定OU DN。

組DN:組DN

組屬性:成員



這篇文章可以幫助您確定基本DN和組DN值。

確定Active Directory LDAP對象屬性

步驟3.2新增目錄伺服器

按一下Add按鈕以導航到下一步,然後按一下Add directory選項。

主機名/IP地址:配置AD伺服器的IP地址/主機名。

埠:389(Active Directory LDAP埠號)

加密/SSL證書: (可選)要加密FMC與AD伺服器之間的連線,請參閱

文章:驗證通過SSL/TLS進行Microsoft AD身份驗證的FireSIGHT系統上的身份驗證對象

Overvie	w Analysis Po	licies Devices Objects Al	MP						Deploy	A Sys	tem Help	▼ admin v
				Configuration	Users	Domains	Integration	Updates	Licenses 🔻	Health 🔻	Monitoring	• Tools •
Serve	ertest											😢 Cancel
Enter a de	scription											
Director	Realm Configur	ation User Download										
	Edit directory		? ×								G	Add directory
URL (Hos	Hostname / IP	192 168 10 11						Encryptio	n			
192.168.1	Address	192.100.10.11						none				08
	Port	389										
	Encryption	○ STARTTLS ○ LDAPS ④ None										
	SSL Certificate	 O 										
		ок	Test Cancel									

按一下Test按鈕以驗證FMC是否能夠連線到AD伺服器。

步驟3.3修改領域配置

導航到領域配置以驗證AD伺服器的整合配置,您可以修改AD配置。

步驟3.4下載使用者資料庫

導航到User Download選項,從AD伺服器獲取使用者資料庫。

啟用此覈取方塊可下載Download users and groups,並定義有關FMC聯絡AD下載使用者資料庫頻率的時間間隔。

選擇組並將其放入要為其配置身份驗證的Include選項。

Directory Realm Configuration User Download			
Download users and groups Begin automatic download at 12 AM America/New York Repeat Every 24 d Download Now	▼ Hours		
Available Groups 😋	Groups to Include (1)	Groups to Exclude (0)	
▲ Search by name	to de to	None	
	Enter User Inclusion	Add Enter User Exclusion	Add

如圖所示,啟用AD狀態:

Overview Analysis	Policies Devices	Objects AM	Р					Deploy 01 Sys	tem He	lp v admin v
Dashboards Report	ng Summary 🔻									
Cisco CSI Realms	Identity Sources	eStreamer	Host Input Client	Smart Software Satellite	2					
								Comp	are realms	New realm
Name			Description	Domain	Туре	Base DN	Group DN	Group Attribute	State	
servertest-1				Global	AD	dc=servertest,dc=com	cn=TAC,ou=Security-Tea	r member		ቲ 🦉 🛅 🖯

步驟4.配置身份策略

身份策略執行使用者身份驗證。如果使用者未進行身份驗證,則拒絕訪問網路資源。這會對組織的 網路和資源實施基於角色的訪問控制(RBAC)。

步驟4.1強制網路門戶(主動身份驗證)

Active Authentication在瀏覽器中要求輸入使用者名稱/密碼,以標識允許任何連線的使用者身份。 瀏覽器使用身份驗證頁面對使用者進行身份驗證,或使用NTLM身份驗證進行靜默身份驗證。 NTLM使用Web瀏覽器來傳送和接收身份驗證資訊。主動身份驗證使用各種型別來驗證使用者的身份。不同型別的身份驗證包括:

- 1. HTTP基本資訊:在此方法中,瀏覽器會提示輸入使用者憑證。
- 2. NTLM:NTLM使用Windows工作站憑據,並通過Web瀏覽器與Active Directory進行協商。您需 要在瀏覽器中啟用NTLM身份驗證。使用者身份驗證透明進行,不提示輸入憑據。它為使用者 提供單點登入體驗。
- HTTP協商:在此型別中,系統嘗試使用NTLM進行身份驗證。如果失敗,則感測器使用HTTP Basic身份驗證型別作為回退方法,並提示一個使用者憑據對話方塊。
- 4. 「HTTP響應」頁:這與HTTP基本型別類似,但是,在此提示使用者將身份驗證填寫到可自 定義的HTML表單中。

每個瀏覽器都有啟用NTLM身份驗證的特定方式,因此它們遵循瀏覽器指南以啟用NTLM身份驗證。

要安全地與路由感測器共用憑據,需要在身份策略中安裝自簽名伺服器證書或公開簽名的伺服器證

書。

Generate a simple self-signed certificate using openSSL -

- Step 1. Generate the Private key openssl genrsa -des3 -out server.key 2048
- Step 3. Generate the self-signed Certificate. openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.crt

導航到Policies > Access Control > Identity。按一下Add Policy,為策略指定名稱並儲存。

Overview Analysis Policies Devices Objects	AMP			Deploy 🛕 System Help 🔻 admin 🔻
Access Control > Identity Network Discovery App	plication Detectors	Correlation Actions •		
				Object Management Access Control
				Compare Policies
Identity Policy	Domain		Status	Last Modified
		New Identity policy	? X	
		Name Identity_Policy	Add a new policy	
<u>.</u>		Description		
		Save	ncel	

導覽至Active Authentication索引標籤,並在Server Certificate選項中按一下圖示(+),然後上傳您在 上一步使用openSSL產生的憑證和私密金鑰。

Overview Analysis	Policies Devices Obje	ects AMP			Deploy 01 System Help 🔻 admin 🔻
Access Control + Identi	ty Network Discovery	Application Detectors	Correlation	Actions v	
Identity_Policy Enter a description					You have unsaved changes 🛛 😭 Save 🛛 🔀 Cancel
Rules Active Authentic	ation				
Server Certificate *	Self_Sign_Cert	v o			
Port *	885	(885 or 1025 - 6553	15)		
Maximum login attempts *	3	(0 or greater. Use 0	to indicate unlimi	ted login attempt)
Active Authentication Res This page will be displayed in Type. System-provided	ponse Page f a user triggers an identity rule	with HTTP Response Page	as the Authentica	tion	
* Required when using Activ	e Authentication				

現在,按一下Add rule按鈕,為Rule指定一個名稱,並選擇作為Active Authentication的操作。定義 要為其啟用使用者身份驗證的源/目標區域、源/目標網路。

選擇在上一步中配置的Realm以及最適合您的環境的身份驗證型別。

Overview Analysis Polic	ies Devices Objects	AMP					Deploy	🗛 System Help 🔻 admin 🕯
Access Control > Identity	Network Discovery Applic	ation Detectors	Correlation Actions •					
Identity_Policy								Save 🛛 🕄 Cancel
Enter a description								
Rules Active Authentication								
	Add Rule					@ 11101 A	? X	Rules
# Name	Name Captive_Portal		✓ Enabled	1	Insert into Catego	ory Y Standard Rul	es 👻	Auth Type
Administrator Rules	Action Active Authentication	n	▼ Realm: Servertest (AD)	Authentication T	ype: HTTP Negotia	te Exclude HTTP User-Agents: No	one	
This category is empty	Zonos Natworks W	AN Tage Dorte				Por	Im & Cottings	
Standard Rules	Zones Networks Vi	LAN Tags Ports				Rea	inn & Settings	
This category is empty	Realm *	Servertest (AD)		- <i>2</i>				
Root Rules	Identify as Special Identi	ities/Guest if authentica	tion cannot identify user					
This category is empty	Authentication Type	HTTP Negotiate		~				
	Application Filters		Available Applications (83) 🖒			Exclude HTTP User-Agents (0)		
	Search by name		Search by name			any		
	A Risks (Any Selected)		ABC	0 -				
	Very Low	19	AdobeAIR	ŏ	Add to Rule			
	Low	40	Advanced Packaging Tool	ŏ				
	🖂 📝 Medium	11	AirPlay	0				
	🖂 🖌 High	6 🗸	Amazon Instant Video	0 -				
	* Required Field							
						Add	Cancel	

強制網路門戶的ASA配置

對於ASA Firepower模組,請在ASA上配置這些命令以配置強制網路門戶。

ASA(config)# captive-portal global port 1055

確保在Identity Policy Active Authentication 頁籤的port選項中配置伺服器埠TCP 1055。

若要驗證活動規則及其命中計數,請運行命令:

ASA# show asp table classify domain captive-portal

💊 注意:Captive portal命令在ASA 9.5(2)版及更高版本中可用。

步驟4.2單點登入(被動身份驗證)

在被動身份驗證中,當域使用者登入並能夠對AD進行身份驗證時,Firepower使用者代理會從AD的 安全日誌中輪詢使用者 — IP對映詳細資訊,並與Firepower管理中心(FMC)共用此資訊。FMC會將 這些詳細資訊傳送到感應器,以便執行存取控制。

按一下Add rule按鈕,為規則指定一個名稱,然後選擇Action作為Passive Authentication。定義要 為其啟用使用者身份驗證的源/目標區域、源/目標網路。

選擇您在上一步中配置的領域,以及最適合您環境的身份驗證型別,如下圖所示。

如果被動身份驗證無法識別使用者身份,可以在此處選擇回退方法作為主動身份驗證。

Overview Anal	ysis Policies Devid	ces Objects AMP				Deploy 01 S	ystem Help 🔻 admin 🔻
Access Control >	Identity Network Di	scovery Application Dete	ctors Correlation	Actions 🔻			
Identity_Po	licy					You have unsaved change	s 🦷 Save 😢 Cancel
Enter a description							
Rulas Activo Aut	thentication						
Rules Active Aut	menucation				A		_
	Editing Rule - Captiv	ve_Portal					? ×
# Name	Name Single_Sign_On		🗹 Enable	d <u>Move</u>			th Type
Administrator Rule	Action Passive Authenti	cation	Realm: Servertest	Authentication Type: HTTP	Negotiate Exclude HTTP Us	er-Agents: None	
This category is em							
Standard Rules	Zones Networks	VLAN Tags Ports				Realm & Sett	tings
1 Captive_Portal	Realm *	Servertest		× 2			'P Negotiate 🥥 🗍
Root Rules	Use active authentica	ation if passive authentication ca	annot identify user				
This category is em							
	* Required Field						
						Save Cano	cel

步驟5.配置訪問控制策略

導航到Policies > Access Control > Create/Edit a Policy。

按一下Identity Policy(左側上角),選擇在上一步中配置的Identify Policy並按一下OK按鈕,如下 圖所示。

Overview Analysis Polici	es Devices Objects	AMP		Deploy 🔍 System Help 🔻 admin 🔻
Access Control + Access Cont	rol Network Discovery	Application Detectors	Correlation	actions *
NGFW_Policy				🔊 Show Warnings
Enter a description				
Identity Policy: None	SSL Policy: None			
	Identity Policy		? ×	Theritance Settings 🕎 Policy Assignments (1)
Rules Security Intelligence			~ ~	
General Settings	Identity_Policy		· · ·	insport/Network Layer Preprocessor Settings
Maximum URL characters to sto	Revert to Defaults	ок	Cancel	nore the VLAN header when tracking connections No

按一下Add rule按鈕新增新規則。導覽至Users,並選擇對其強制執行訪問控制規則的使用者,如下 圖所示。按一下「OK」,然後按一下「Save」以儲存變更。

Overview Anal	vsis Policies	Devices Objects	AMP					Deploy	🛕 System H	Help ▼ a	dmin 🔻
Access Control >	Access Control	Network Discovery	Application Detectors	Correlation	Actions T						
NGFW_Polic	:y									ave 🛛 🕄	Cancel
Enter a description											
Identity Policy: Ide	ntity_Policy	SSL Policy: None									
Rules Securit	Editing Rule -	Allow_LAN_User							? ×	y Assignm	ents (1)
# Filter by Devic	Name Allow_LA	N_User		🗹 Enabled	Move						×
# Name	Action	(✓ IPS: no po	licies Variables	: n/a Files: no inspe	ection Logging: co	onnections: Event V	/iewer			
👻 Mandatory - I	Zones Net	works VLAN Tags	Users Applications	Ports URLs	🔺 ISE Attributes		Inspection	Logging	Comments		
1 Allow LAN L	Available Realms	s Ċ	Available Users	Ċ		Sele	ected Users (2)			R 0	0 B
I MINW_DAN_O	Search by nar	me or value	Search by nam	e or value		8	Servertest/sunil		8	- ·	ø U
🗢 Default - NGF	Special Identi	ities				*	Servertest/admin		6		
2 IPS_test	Servertest									0	08
Default Action										~	\$ 📕
								ок	Cancel		

步驟6.部署訪問控制策略

導航到Deploy選項,選擇Device,然後按一下Deploy選項將配置更改推送到感測器。從消息中心圖示(部署和系統選項之間的圖示)選項監視策略的部署,並確保策略必須成功應用,如下圖所示。

		Deploy 🔒 🔒 Sy	ystem Help 🔻 admin 🔻
C Depl	oy Policies Version: 2015-12-10 09:29 PM		? ×
	Device	Group	Current Version
	NGFW		2015-12-10 09:14 PM
	NGFW Settings: NGFW		
	D Access Control Policy: NGFW_Policy		
	Intrusion Policy: Balanced Security and Connectivity		
	Intrusion Policy: No Rules Active		
	Identity Policy: Identity_Policy		
	ONS Policy: Default DNS Policy		
	Network Discovery		
5	Device Configuration (<u>Details</u>)		
S	Selected devices: 0		Deploy Cancel

步驟7.監視使用者事件和連線事件

當前活動的使用者會話在分析>使用者>使用者部分中可用。

使用者活動監控有助於確定哪個使用者與哪個IP地址相關聯,以及系統如何通過主動或被動身份驗 證檢測使用者。 「分析」(Analysis)>「使用者」(Users)>「使用者活動」(User Activity)

User Activity

Table View of Events > Users

No Search Constraints (Edit Search)

	<u>▼ Time</u> ×	Event ×	<u>Realm</u> ×	<u>Username</u> ×	<u>Type</u> ×	Authentication X Type	IP Address ×
4	2015-12-10 11:15:34	<u>User Login</u>	<u>Servertest</u>	📑 <u>sunil</u>	LDAP	Active Authentication	192.168.20.20
4	2015-12-10 10:47:31	<u>User Login</u>	<u>Servertest</u>	📇 <u>admin</u>	LDAP	Passive Authentication	<u>192.168.0.6</u>

導覽至Analysis > Connections > Events,以監控使用者使用的流量型別。

Overview Analysis Policies Devices Objects AMP Deploy 🔺 System Help 🗸 System Help 🗸													
Co	ntext E	xplorer Connectio	ns • Events Intru	sions • Fil	es 🔹 Hosts 💌	Users • Vulnerabilities •	Correlation • Cust	com v Search					
	Bookmark This Page Report Designer Dashboard View Bookmarks Search												
	Connection Events (switch workflow) Connections with Application Details > Table View of Connection Events > Search Constraints (Edit Search Save Search) Diabled Columns												
vump to 🔻													
			Last Packet ×	Action ×	Initiator IP ×	Initiator User ×	Responder IP ×	Access Control Rule ×	Ingress Interface ×	Egress Interface ×	Count		
1		2015-12-11 10:31:59	2015-12-11 10:34:19	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1		
4		2015-12-11 10:31:59		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	74.201.154.156	Allow LAN User	Inside-2	Outside	1		
4		2015-12-11 09:46:28	2015-12-11 09:46:29	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1		
4		2015-12-11 09:46:28		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1		
4		2015-12-11 09:46:07	2015-12-11 09:46:58	Allow	192.168.20.20	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1		
4		2015-12-11 09:46:07		Allow	192.168.20.20	📇 sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1		
4		2015-12-11 09:45:46	2015-12-11 09:46:36	Allow	192.168.20.20 <u>192.168.20.20</u>	Sunil (Servertest\sunil, LDAP)	173.194.207.113	Allow LAN User	Inside-2	Outside	1		
Las	t login o	n Thursday, 2015-12-10 at	11:17:25 AM from 10.65.3	9.169 Right-clic	k for menu						alialia		

驗證和疑難排解

導覽至Analysis > Users,以驗證與流量相關的使用者驗證/驗證型別/使用者 — IP對應/存取規則。

驗證FMC和使用者代理之間的連線(被動身份驗證)

Firepower管理中心(FMC)使用TCP埠3306,以便從使用者代理接收使用者活動日誌資料。

若要確認FMC服務狀態,請在FMC中使用此命令。

admin@firepower:~\$ netstat -tan | grep 3306

在FMC上運行資料包捕獲,以驗證與使用者代理的連線。

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 3306

導覽至Analysis > Users > User Activity,以驗證FMC是否從使用者代理收到使用者登入詳細資訊。

驗證FMC和Active Directory之間的連線

FMC使用TCP埠389從FMC中檢索使用者資料庫 Active directory。

在FMC上運行資料包捕獲以驗證與Active Directory的連線。

admin@firepower:~\$ sudo tcpdump -i eth0 -n port 389

確保FMC領域配置中使用的使用者憑據具有獲取AD使用者資料庫的足夠許可權。

驗證FMC領域配置,並確保已下載使用者/組且正確配置使用者會話超時。

導航到Message Center > Tasks,並確保任務使用者/組下載成功完成,如下圖所示。

				Dep	loy	System	stem	Help	adm	in
Deploy	ments	🔥 Health	Tasks						۲	?
20+ t	otal	0 waiting	0 running	0 retrying	20+	success	1 fa	ailure		
V LDA	 LDAP Download - Global Download users/groups from servertest-1. LDAP download successful: 1 groups, 0 users downloaded 									
V LDA	P Downlo wnload cessful:	ad - Global users/grou 1 groups, 5	u ps from se users downl	ervertest-1. oaded	LDAP	downloa	d		4m 52s	×

檢驗Firepower感測器與終端系統之間的連通性(主動身份驗證)

對於主動身份驗證,請確保在FMC身份策略中正確配置證書和埠。預設情況下,Firepower感測器 在TCP埠885上偵聽主動身份驗證。

驗證策略配置和策略部署

確保在身份策略中正確配置領域、身份驗證型別、使用者代理和操作欄位。

確保身份策略與訪問控制策略正確關聯。

導航到Message Center > Tasks,並確保策略部署成功完成。

分析事件日誌

連線和「使用者活動」事件可用於診斷使用者登入是否成功。這些事件

還可以驗證對流應用了哪個訪問控制規則。

導航到Analysis > User以檢查使用者事件日誌。

導航到Analysis > Connection Events以檢查連線事件。

相關資訊

• 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。